# The social engineering framework para el aseguramiento de PYME

Alejandro Correa Sierra
Carlos Andres Orrego Ossa.
Noviembre 2015.

Universidad Eafit.
Departamento de Sistemas.
Trabajo de Grado

**Resumen**

El trabajo plantea un aporte al framework de ingeniería social (The Social Engineering Framework) para la evaluación del riesgo y mitigación de distintos vectores de ataque, por medio del análisis de árboles de ataque. Adicionalmente se muestra una recopilación de estadísticas de ataques realizados a compañías de diferentes industrias relacionadas con la seguridad informática, enfocado en los ataques de ingeniería social y las consecuencias a las que se enfrentan las organizaciones. Se acompañan las estadísticas con la descripción de ejemplos reales y sus consecuencias.

**Tabla de Contenidos**

**Lista de figuras**

# 1 Introducción

Con el desarrollo de nuevas tecnologías las cuales son vendidas al público con fallas de seguridad, desarrollo de medios de comunicación masivos donde los usuarios publican información confidencial y permiten a personas con objetivos ilegales obtener información de usuarios para ser utilizada según sus propios beneficios, se ve la necesidad de recomendar un conjunto procedimientos abiertos para la evaluación de vulnerabilidades de ingeniería social, con el objetivo de evaluar el nivel de seguridad de la información de las organizaciones en poder los usuarios o empleados.
Son diferentes los medio por los cuales, un empleado puede entregar información sin siquiera identificar la fuga de está comprometiendo la seguridad de la información.
para ilustrar lo anterior presentamos estadisticas de ataques de ingenireia social a traves de paginas web, para que las organizaciones tomen la iniciativa de realziar procedimientos de manejo de información por parte de sus empleados, lo cual permita mitigar los riesgos de ataques de ingenieria social.
Actualmente los ataques tecnológicos a las organizaciones no necesariamente se realizan directamente sobre los sistemas, se ha tenido una experticia por parte de los atacantes en realizar un proceso diferente para el acceso a información confidencial de las organizaciones, esto se realiza a través del eslabón más débil de una organización que son la personas por medio de ingeniería social. Este método, de bajo costo de ejecución y gran eficiencia a demostrado ser uno de los más eficaces para el robo de información, y la primera puerta de entrada a los sistemas tecnológicos.

Para ilustrar lo anterior se plantea el caso de un empleado descontento que obtiene su "venganza" realizando un ataque de ingeniería social que inicia con la obtención, a través de engaño desde la mesa de ayuda, de usuarios de red y claves de acceso, adicionalmente trata de obtener la IP de sus estaciónes de trabajo y así poder instalar un keylogger para obtener contraseña de usuario de base de datos de los clientes restringidos y finalmente usa herramienta HTTP tunneling comercial que permite a los usuarios eludir medidas de seguridad[1].
En Colombia, el delito informático está regido y penado por la "ley 1273 DE 2009"[2]
la cual decretó que se multará con penas de prisión y multa económica a quien desee acceder a los sistemas de información o información confidencial si tener una autorización,

[1] https://www.sans.org/reading-room/whitepapers/engineering/story-disgruntled-employee-revenge-1548
[2] http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

o impida el funcionamiento correcto de un sistema de información teniendo algún tipo de manipulación (Borrado o eliminación) de información.

Para este tipo de ataques se ha estado trabajando en un framework cuyo objetivo es crear un repositorio de información profesional de seguridad, pruebas de penetración para tener un conocimiento de los ataques más utilizados hoy en día.

La ingeniería social consiste en obtener información confidencial a través de la manipulación de usuarios legítimos, los cuales son el eslabón más débil en cualquier sistema de seguridad.

De acuerdo a Kevin Mitnick, en su libro "the art of deception" la clave de la seguridad informática no corresponden a mecanismos de seguridad implementados a nivel de hardware y software sino la capacidad de los usuarios de cumplir correctamente las políticas de seguridad y hacerlas cumplir.

Existen 4 principios básicos en la ingeniería social:

- Todos queremos ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir No.
- A todos nos gusta que nos alaben[3].

Con la utilización de estos 4 principios descritos, se podrá, en organizaciones donde la cultura de seguridad informática no este correctamente implementada y no se cuenten con políticas ni procedimientos divulgados, vulnerar la seguridad implementada a nivel de hardware y software sin costosos mecanismos ni altos conocimientos tecnológicos.

Asimismo, si nos ubicamos en un contexto actual, es fácil identificar personas a las cuales se les puede realizar ingeniería social, esta personas pueden ser conocidas o simplemente empleados de una empresa, ya que a través de las redes sociales es la principal fuente para realizar este método de sustracción de información por el contenido que se maneja en ellas.

[3] http://www.cnet.com/news/social-engineering-101-mitnick-and-other-hackers-show-how-its-done/

De igual manera se debe de tener un conocimiento específico para realizar los ataques, y realizar una buena estrategia de comunicación de información (Suplantación) al usuario para que este pueda ser vulnerable en dicho proceso o ataque informático[4].

De entender bien la metodología de los diferentes tipos de ataque de ingeniería social, las personas interesadas en estudiar el tema puede tener unas bases para implementar mecanismos de defensa que prevengan la vulneración de la seguridad.

[4] http://www.scis.nova.edu/~cannady/ARES/mitnick.pdf

# 1. Formulación Del Problema

## 1.1 Justificación

Dada la creciente necesidad de las compañías de realizar una protección de su infraestructura debido a la alta tasa de ataques informáticos realizados alrededor del mundo, y el creciente riesgo por la migración a tecnologías inestables o con fallas de seguridad realizadas por empresas con poca conciencia en temas de seguridad informática, se pretende elaborar un marco de trabajo como aporte al marco de trabajo de ingeniería social que permita a las organizaciones PYMES evaluar su estado de vulnerabilidad frente ataques del tipo de Ingeniería Social e implementar posibles soluciones a las mismas[5].

Se realizará un aporte el cual sirve como marco de referencia para empresas que busquen minimizar sus vulnerabilidades, riesgos e impactos por ataques de ingeniería social y un medio para mantener a sus empleados conscientes de la posibilidad de pérdida de información por parte de personal no autorizado.

## 1.2 Objetivos

### 1.2.1 General.

Crear un conjunto de procedimientos ABIERTOS para la evaluación de las vulnerabilidades de ingeniería social, aportando al framework de ingeniería un árbol de decisiones del atacante y posibles mitigaciones, esto deberá contener la perspectiva social y la perspectiva técnica con ejemplos concretos documentados.

### 1.2.2 Específicos.

- Detallar algunos tipos de ataques sé que presentan a través de la ingeniería social en las industrias y datos históricos de ataques.

[5] http://www.welivesecurity.com/la-es/2014/12/18/tendencias-cibercrimen-predicciones-2015/

- Detallar pasos para la identificación de vulnerabilidades relacionadas con ingeniería social.
- Defini un conjunto de procedimientos para la evaluacion de vulnerabilidades frente a taques de ingeniería social
- Clasificación de criticidad e impacto de posibles resultados.
- Definición de planes de acción para la mitigación y disminución de las vulnerabilidades identificadas

### 1.3 Importancia aporte Ingeniería Social

La investigación en cuanto tema de ingeniería social nos llevara a vernos beneficiados y a obtener un alto conocimiento sobre la implementación del análisis de seguridad, su revisión o supervisión lo cual aporta al framework de ingeniería social para que su implementación.

Este proyecto está orientado principalmente a las PYMES y usuarios de las tecnologías de información en general, que se concienticen del manejo de la seguridad de la información, ya que si se contara con herramientas que le permitirán implementar el procedimiento de detección, análisis y corrección de vulnerabilidades minimiza la posibilidad de pérdida de información y denegación de servicios por ataques realizados por hackers informáticos.

## 2 Metodología

Para la elaboración del trabajo utilizaremos la siguiente metodología.

- Recolección de la información
- Análisis de la Información recolectada
- Realización de procedimiento para la mitigación de vulnerabilidades
- Estudio de estadística y casos históricos

## 3 Estado del Arte

De acuerdo a estudios realizados, en los últimos años, se está viendo un incremento constante, sobretodo en Colombia, en la realización de ataques informáticos a empresas o personas naturales. Este incremento se debe principalmente a migración a nuevas tecnologías informáticas como mayores capacidades de almacenamiento y procesamiento de datos con relativos bajos costos, almacenamiento en línea (nube), desconocimiento de los nuevos sistemas de ataque o la falta de formación para enfrentarlos. De acuerdo con un artículo presentado en la página web de Colombia Digital, empresa organización dedicada a promover el uso y apropiación de las tecnologías de información y las comunicaciones, en beneficio del desarrollo social y económico, un estudio realizado por ESET afirma que

el 41% de las organizaciones Colombianas han sufrido ataques de tipo malware. De acuerdo al reporte presentado, los principales ataques utilizados son la vulnerabilidad de los sistemas, la infección de malware, fraudes, suplantación de identidad y ataques DOS [6].

Según la compañía de seguridad informática Digiware, compañía latinoamericana dedicada a la detección y prevención de ataques informáticos, Colombia es actualmente el país de habla hispana que actualmente más ataques informáticos sufre, seguido por países como Argentina y Peru[7].

El alto costo en tecnologías de prevención y la incredulidad de dueños de pequeños y medianos negocios de que sus organizaciones algún día puedan estar bajo ataque, favorecen a que los grupos o individuos con objetivos ilegales, están ganando dicha batalla.

Uno de los vectores de ataque más utilizados actualmente, debido a que requiere una baja inversión (o ninguna) en tecnologías para la realización del ataque, el bajo conocimiento técnico requerido para la realización y las altas tasas de éxito que registra son los ataques de Ingeniería social.

### 3.1 Ingeniería social

Para comprender que es, como afecta y se puede defender la información de las organizaciones de ataques de Ingeniería social requerimos conocer sus aspectos fundamentales, tipos de ataques, árboles de decisiones y métodos de mitigación de vulnerabilidades.

¿Qué es la ingeniería social?. Podemos encontrar diferentes definiciones, entre ellas:

- la ingeniería social según el diccionario Merriam Webster es la gestión de los seres humanos en interactuar en un lugar con una función en una sociedad, utilizando las relaciones humana para alcanzar una meta en específico[8].

[6] http://colombiadigital.net/actualidad/noticias/item/7289-perspectiva-de-la-seguridad-informatica-en-latinoamerica.html
[7] http://www.digiware.net/?q=es/content/sala-de-prensa
[8] https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-1365).

- Ingeniería Social es la manipulación intencionada individual o de grupo para obtener información o efectuar obtener información o afecto por determinado comportamiento, Puede implicar o el uso de tecnologías, pero utiliza principalmente el engaño[9].

De las definiciones referenciadas, podemos concluir que los ataques de ingeniería social, se basan en la manipulación de personas, con el objetivo de conseguir una meta, esta meta pueden ser, entre muchas, información confidencial, credenciales de acceso, cuentas bancarias o permisos especiales.

La ingeniería social, es un método de ataque informático altamente utilizados debido a que es difícil de detectar, cuenta con la ventaja de que no importa cuánto dinero y esfuerzo se invierta para mitigar las probabilidades de ataques, no es posible estar protegido en su totalidad, ni se cuenta con un medio hardware o software para asegurar que no se realizan ataques.

Los tipos de ataque de ingeniería social se dividen en varias categorías dependiendo del grado de conocimiento que tiene las víctimas. Los tipos de divisiones[10] son:

Técnicas pasivas

- Observación: Consiste como su nombre lo indica en la obtención de información por medio de la observación: búsqueda en redes sociales, páginas web, directorios, entre otros

Técnicas activa no presenciales

- Recuperar la contraseña: Está comúnmente asociada a la recuperación de contraseñas por medio de las respuestas a las preguntas de seguridad en una página o red social
- Ingeniería Social y Mail: Campañas de correo electrónico con el objetivo de que la víctima suministre información
- IRC u otros chats: suplantación o solicitud de información confidencial en chats
- Teléfono: llamadas telefónicas suplantando personal o solicitando información confidencial

[9] http://csrc.nist.gov/organizations/fissea/2006-conference/Tuesday300pm-OLeary.pdf
[10] http://hackstory.net/Ingenier%C3%ADa_social

- Carta y fax

Las técnicas no presenciales, son utilizadas generalmente como punte para la utilización de ataques informáticos técnicos como pueden ser: la ejecución o envío de virus informáticos, ataques de SQL inyección, o la inyección de código malicioso entre otros.

Técnicas presenciales no agresivas

- Buscando en La basura
- Mirando por encima del hombro
- Seguimiento de personas y vehículos
- Vigilancia de Edificios
- Inducción
- Entrada en Hospitales
- Acreditaciones
- Agendas y teléfonos móviles
- Desinformación

Métodos agresivos

- Suplantación de personalidad
- Chantaje o extorsión
- Impersonación
- Presión psicológica

También podemos dividir los diferentes tipos de ataque de ingeniería social dependiendo del método de acercamiento que se tienen con la víctima:

- Ataque basado en la interacción humana: son aquellas que involucran la interacción con seres humanos de cualquier forma. Comúnmente utilizada para realizar ataques de suplantación de identidad de soporte técnico y usuarios importantes
- Ataque Basado en la utilización de medios electronicos: Son los ataques que dependen de la utilización de computadores o red de datos. Comúnmente utilizados en ataques de phising, correo falsos o ataques de pop-ups en navegadores.
- Ataque Basado en ataques a dispositivos móviles: como su nombre lo indica, con ataques realizados sobre dispositivos móviles. Como por ejemplo: aplicaciones maliciosas o keyloggers entre otros[11].

[11] https://aspen.eccouncil.org

Con el objetivo de proteger la información, es importante identificar las diferentes etapas empleadas por los atacantes para la realización de un ataque de ingeniería social. Si identificamos las fases podemos desarrollar estrategias que impidan fuga de información que faciliten el ataque a nuestras organizaciones. En general, las fases de un ataque de ingeniería social[12] son:

- Investigar el objetivo: Esta fase como su nombre lo indica, consiste en la búsqueda de información del objetivo. Para esta etapa se pueden realizar actividades como: búsqueda en la web del objetivo, revisión de dumpster diving, redes sociales o incluso algunas más técnicas como escaneo de información a las páginas web de la compañía. Actualmente se encuentran adicionalmente herramientas de fácil utilización que obtinen la mayor cantidad de información a partir de una página web.
- Selección de la víctima: basados en la información obtenida en la etapa anterior, se procede a seleccionar el eslabón más débil de la compañía o aquella persona que tiene la información u objetivo que estamos buscando
- Establecer relación: se establece una conexión con la víctima, puede ser una llamada telefónica, un correo, entre otros
- Explotar la relación establecida: Aprovechar la conexión establecida y cumplir con la finalidad del ataque.

Sin embargo, es importante aclarar que la ingeniería social no es una técnica definida, y que sus fases son cumplidas en la totalidad de los casos. Según Jacqueline Tangarife, gerente de Security Solutions & Education, empresa que es la representante exclusiva para Colombia de EC-Council Academia

*"La ingeniería social no es una técnica cuadriculada. Depende de la malicia del atacante, así como de la que tenga la víctima. Se pueden utilizar infinidad de argucias y mañas para lograr la información que se necesita: desde sobornos a amigos y familiares para que faciliten el acceso a ella, hasta preguntas sueltas en ambientes de esparcimiento, correos electrónicos aparentemente inofensivos que hacen preguntas sencillas y cuyas respuestas interesan a quien solicita la información[13]"*

[12] https://sin.thecthulhu.com/library/security/social_engineering/The_Art_of_Human_Hacking.pdf
[13] http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/

Entender los diferentes métodos de ataque puede ser fundamental al momento de definir una estrategia para defendernos. También es importante estar en constante monitoreo de los diferentes alertas que se pueden generar en la organización para determinar que estamos bajo ataque.

### 3.2 Histórico de ataques

Como se ha venido hablado los ataques informáticos se pueden observar a traves de algunas estadísticas que presentaron en el 2014 en los países latinoamericanos, donde se presentaron diferentes tipos de ataques, entre los cuales están:

- Campaña diseñada con fines de ciberespionaje utilizando programas maliciosos con la capacidad de comprometer equipos basados en Sistemas Mac OS X, Linux, iOS (iPad/iPhone) y Android[14].

- Machete es una campaña de ciberespionaje ataca países de Latinoamérica o sus embajadas y representantes en otros países del mundo[15], este tipo de fraude tipicamente involucra la promesa de dinero o premio a la victima, la cual debe de pagar una suma para poder obtener dicho beneficio.
- Mundial de futbol 2014, fue una campaña que buscaban mediante ingeniería social o phishing engañar a los usuarios con promociones para viajar "gratis" a Brasil o la venta de entradas a los diferentes partidos[16].

- Reaparición de malware basado en macros office, en Colombia encontramos el caso de la DIAN, donde utilizaron correos electrónicos para hacer creer a los usuarios que estaban acusados de evasión fiscal por lo tanto deberían de abrir documentos anexos[17].

### 3.3 Estadísticas

Estos ataques fueron algunos de los más comunes durante 2014 en Latinoamérica, estos ataques se registraron o presentaron de diferentes maneras como:

---

[14] http://latam.kaspersky.com/mx/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/kaspersky-lab-descubre-la-m%C3%A1scara-una-de-las-

[15] http://www.viruslist.com/sp/weblog?weblogid=208188998

[16] http://www.viruslist.com/sp/weblog?weblogid=208188789

[17] http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/blog-de-kaspersky/2014/Malware_DIAN

| Ranking mundial | País | % de usuarios con intentos de infección | Nº de incidentes |
|---|---|---|---|
| 38 | Brasil | 32.0% | 22122995 |
| 63 | Perú | 28.7% | 4537175 |
| 64 | Panamá | 28.5% | 929976 |
| 74 | México | 27.0% | 17514481 |
| 80 | Honduras | 26.5% | 458438 |
| 90 | El Salvador | 25.4% | 439970 |
| 92 | Nicaragua | 24.9% | 310517 |
| 95 | Ecuador | 24.6% | 3157211 |
| 97 | Colombia | 24.4% | 4991622 |
| 98 | Chile | 24.2% | 1813276 |
| 99 | Guatemala | 24.2% | 822242 |
| 112 | República Dominicana | 22.8% | 435710 |
| 125 | Costa Rica | 21.6% | 588932 |
| 132 | Argentina | 21.2% | 1375126 |
| 148 | Uruguay | 19.6% | 175873 |
| 165 | Paraguay | 17.9% | 238189 |
| 232 | Cuba | 7.9% | 30586 |

*Figura 1.* Ranking ataques Latinoamérica[18].

"Al lanzar ataques en línea, los criminales utilizan diferentes tipo de sitios Web donde alojan los programas de código malicioso. A veces estos sitios Web son legítimos pero comprometidos previamente, de modo que el propietario del sitio no está al tanto del incidente. En otras ocasiones los criminales usan los sitios Web gratuitos o comerciales pero dedicados en un 100% al crimen, es decir no hospedan nada más que malware. [19]. "

Como podemos ver la web es uno de los lugares a través del cual se realizan más delitos informáticos y Latinoamérica está muy expuesta a los ataques informáticos, por lo que presentamos una estadística de los dominios que más se utilizan para esta práctica[20]:

[18] http://latam.kaspersky.com/mx/analisis2014pronosticos2015LatAm

[19] http://latam.kaspersky.com/mx/analisis2014pronosticos2015LatAm

| Dominio malicioso | Cantidad de malware registrado |
|---|---|
| u***s.cdneurope.com | 7674901 |
| ads.***nime.net | 4197121 |
| cdn-***s.com | 2113674 |
| vitri***sa.com | 1228734 |
| app.corespar***.com | 985476 |
| ads.***tspace.com | 895990 |
| applicationgr***.net | 853516 |
| ***arcasmo.com | 792946 |
| mo***astube.com | 791593 |
| fo***-download.net | 620690 |
| con***ecidade.com | 616730 |
| ***gendelgolfo.com.mx | 573737 |
| ***icaevestibular.com.br | 559954 |
| ***pda.com | 481447 |
| dy***winab0s2.cloudfront.net | 440848 |
| ox.r***arch.me | 420776 |
| links***elho.com | 354936 |
| w***.wifirouter.net | 332254 |
| adult***ssite.net | 319003 |

*Figura 2.* Registro de ataque a través de páginas web[21].

De la anterior observamos que según los tipos de ataques y los métodos a través de los cuales se realizan los delitos informáticos van de la mano antecedida de un trabajo de ingeniería social para ver qué tipo de público o personas en específica puede caer en el engaño.

### 3.4 Comportamiento de los ataques

Un atacante puede aprovechar de los siguientes comportamientos y la naturaleza de las personas cometer ataques de ingeniería social.

- la naturaleza humana hace que la confianza se convierte en la base principal para los ataques de ingeniería social, por lo que las empresas deben de concientizar a sus empleados de tener cuidado con la información que se comunica a las personas, e identificar.

[21] http://latam.kaspersky.com/mx/analisis2014pronosticos2015LatAm

- Las tecnologías implementadas en las organizaciones de igual manera que la naturaleza humana se convierte de una puerta abierta para los ataques de ingeniería social, ya que por medio de ellas se puede transmitir información confidencial o personal a través de la cual se puede llegar a información sensible de las organizaciones, por lo que de igual manera se debe de concientizar a las personas al bueno huso de las herramientas tecnológicas (tiene un punto a favor ya que los sistemas tecnológicos cuentan con seguridad, sin embargo no son totalmente seguros).

### 3.5 Prevenciones y mitigación

Como se mencionó en temas anteriores, no es posible la mitigación de los riesgos ni la eliminación completa de las vulnerabilidades de nuestra información, sin embargo es posible minimizar la exposición de nuestra información si implementamos mecanismo que impida la filtración de información confidencial. A continuación se recomendarán algunos de los que se consideran fundamentales para impedir ataques de ingeniería social[22].

- Crear una cultura de protección de la información
- Ser consciente del valor de la información de la compañía y sobretodo el valor de la información que vamos a compartir
- Mantener el software del sistema actualizado y en sus últimas versiones.
- desarrollar scripts que determinen las respuestas que deban tener empleados sobre solicitudes de información
- Implementar auditorias de Ingeniería social
- Comprender cómo operan las auditorías de ingeniería social
- Establecer metas de auditoria
- Que debe y no debe ser incluido en las auditorías
- Seleccionar el mejor auditor o el que más convenga dependiendo de nuestro negocio o información.

Con estos principios fundamentales definidos, se procedera a la creación de un marco de trabajo que permita a las organizaciones evaluar el nivel de protección contra ataques de ingeniería social y establecer mecanismos para la mitigación en una primera fase de estos riesgos[23].

---

[22] https://sin.thecthulhu.com/library/security/social_engineering/The_Art_of_Human_Hacking.pdf
[23] http://www.scribd.com/doc/184891011/CEHv8-Module-09-Social-Engineering-pdf#scribd

### 3.6 Framework

El concepto de framework se define como marco de trabajo (infraestructura digital) en el cual hay un patrón o esqueleto de un esquema de desarrollo o implementación de una aplicación por medio del cual puedo dar seguridad de acceso a los desarrollos realizados.

El objetivo de los framework es ofrecer una funcionalidad a través de patrones y características de cohesión y acoplamiento, con la construcción de piezas y objetos para su funcionamiento, el framework que se esta trabajando contiene una arquitectura basada en un modelo, una vista y un controlador para su funcionamiento[24]:

- El modelo maneja las operaciones lógicas y manejo de información
- La Vista maneja la interfaz gráfica con la cual interactúan los usuarios finales
- El controlador gestiona el acceso al desarrollo (Archivos, Scripts y/o Programas)

Los ataques a través de ingeniería social han sido un problema para las compañías, ya que no cuentan con un método por medio del cual se pueda minimizar la exposición frente a este tipo de ataques.
La creación de marco de trabajo de ingeniería social se encuentra enfocado a los métodos de ataques a las personas y organizaciones en los cuales se tiene en cuenta las siguientes etapas:

- Recopilación de información: este se debe de invertir un buen tiempo de investigación con el fin de identificar probables respuestas, definir metas, familiarizarse con la persona y plantearse un objetivo para el ataque.
- Establecer relaciones con víctima: Punto crítico para el ataque ya que se debe de enlazar el objetivo con el nivel de cooperación de la víctima, con el objetivo de crear un perfil falso a través de redes sociales, correo o telefónicamente para poder ejecutar las acciones.
- Explotación: es la etapa en la que se realiza divulgación de información para obtener los accesos por parte del atacante esto se puede realizar a través revelación de contraseñas por teléfono, por medio de USB, apertura de archivos entre otros.
- Ejecución: se logra el objetivo del ataque.

[24] https://es.wikipedia.org/wiki/Framework

El framework de ingeniería social (social-engineer.org) se basa en ataques como Phishing, Vishing, SMiShing entre otro, sin embargo no se ha realizado un análisis dentro del framework de incluir tipos de mitigaciones para los tipos de ataques que se incluyeron en el framework[25].

### 3.7 Marco de referencia ITIL

"ITIL (*IT Infrastructure Library*, biblioteca de infraestructura de TI) = Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos"[26]

ITIL en cuanto a la gestión de seguridad de la información no habla que se debe de tener 3 pilares fundamentales como lo son la confidencialidad, integridad y disponibilidad de la información solo para las personas autorizadas dependiendo del tipo de funciones en la organización.

la gestión de seguridad según el marco de referencia vela por que la información sea correcta y siempre esté a disposición del negocio y pueda ser utilizada por las personas de adecuadas, teniendo objetivos definidos por políticas se seguridad sobre la información, aseguramiento de estándares y minimizar los riesgos en cuanto al servicio de continuidad del negocio.

Con la guia del marco de referencia de ITIL para la implementación del framework de ingeniería social desde nuestro punto de vista creemos que es necesario para la aseguramiento de información ya que a través de la ingeniería social el objetivo es acceder a la información sensible de las compañías, con la guía de este marco de referencia se puede mitigar los impactos y riesgos de pérdida de información de las organizaciones[27].

Adicionalmente podemos tener el aporte de la norma La ISO 27001:2005 la cual nos brinda un sistema de gestión de seguridad de la información (SGSI) para el mejoramiento

---

[25] http://www.social-engineer.org/framework/attack-vectors/attack-cycle/

[26] http://www.magazcitum.com.mx/?p=50#.VjgzE7cvfIU

[27] http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_seguridad/vision_general_gestion_de_la_seguridad/vision_general_gestion_de_la_seguridad.php

de los procesos de las compañías, en cuanto a implementación, operación, seguimiento, revisión y manternimiento

# 4 Definición términos claves

## 4.1 Riesgo

Debemos de dejar claro que todas las organizaciones están expuestas a delitos informático (directamente en en herramientas tecnológicas o a través del personal de la compañía) lo que hace que cada una de ellas adquiera una serie de riesgos por el tipo de información que manejan para cualquier industria.

El riesgo lo definimos como una posibilidad de amenaza frente información que tenemos expuesta sea a través de tecnología o información que manejan a nivel de usuarios, el riesgo puede tener un impacto muy alto si va de la mano de la vulnerabilidad (que tan expuesta está la información) pero si estas se presentan por separada podemos decir que el riesgo de la información se reduce para lo debemos de tener en cuenta las debilidades y vulnerabilidades frente a la información expuesta para luego poder tomar medidas de aseguramiento de la información para que los riesgos no se materialicen[28].

Los riesgo a través de la ingeniería social son catalogado por las organizaciones como de baja importancia, sim embargo con el aporte al framework de ingeniaria social es factible obtener el acceso a información confidencial a través del primer eslabón más débil que son las personas o usuarios de una organización[29], por medio de (Influenciar, manipulalr o engañar a las personas).

## 4.2 Impacto

Lo podemos definir como huella o efecto producido por un evento presentando en este caso a pérdida de información de una organización de cual equipo de industria

El impacto de los ataques a través de ingeniería social se catalogan como importantes ya que en estos se puede presentar pérdida de robo de información crítica para la compañía (Reportes de nómina en una organización) la cual puede ser confidencial y a través de la cual se puede llegar a perder reputación y dar ventajas competitivas en las diferentes industrias[30].

---

[28] http://www.ecured.cu/Ingenier%C3%ADa_social
[29] http://www.magazcitum.com.mx/?p=1173#.Vjz5h7cvfIU
[30] http://apuntesdeinvestigacion.upbbga.edu.co/wp-content/uploads/ESI-Luis-Eduardo-Pati%C3%B1o-Dur%C3%A1n.pdf

El impacto representa perdida la confidencialidad, integridad y disponibilidad de la información crítica importante para las organizaciones[31].

Para lograr tener una mitigación del impacto de pérdida de información provocado por los diferentes ataques (en este caso ingeniería social) se debe tener conocimiento de la manera de cómo se generan este tipo de ataques y cuáles son los posibles puntos débiles para reforzar la seguridad, en el caso de ingeniería social se realizan campañas de comunicación de información personal por medio de la cual se puedan llegar a acceder a información crítica de la compañía[32].

### 4.3 Vulnerabilidad

Se presenta cuando un atacante descubre que hay alguna falla en la planificación, implementación y configuración de alguna aplicación o sistema operativo, y la podemos utilizar para violar la seguridad.

Las organizaciones de cualquier tipo de industria es vulnerable de una o otro manera, y actualmente la mayoría de las organizaciones sean grandes, pequeñas o medianas empresas cuentan con apoyo tecnológico el cual hace que sea vulnerable a través a de herramientas de hackeo o a través de las personas que laboran en las mismas, por lo que esto hace que a través de un correo electrónico, una llamada telefónica pueda tener acceso una persona externa a la organización esto a través ingreso a la red y ataques que puedan vulnerar la seguridad[33].

En las medianas y pequeñas empresas los ataques de ingeniería social son un poco menos efectivos que en las grandes ya que el volumen de sistemas de información, sin embargo no deja de ser menos importante ya que todas manejan información confidencial según su industria[34].

---

[31] http://veritasonline.com.mx/ingenieria-social-prevenga-el-fraude/

[32] https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

[33] http://es.slideshare.net/roberth.chavez/gestin-del-riesgos-de-seguridad-de-la-informacin

[34] http://www.magazcitum.com.mx/?p=1173#.Vjz5h7cvfIU

## 4.4 Ataques informáticos

Se define ataque informático, a el intento obtener acceso, impedir el correcto funcionamiento o inutilizar otro sistema informático. Actualmente los ataque informáticos, pueden ser catalogados en muchas categorías dependiendo del medio de ataque o el objetivo deseado, ataques de denegación de servicios, sobre paginas o servicios web, ataques de inyección de código, para bases de datos, ataques de hombre en el medio para la obtención de información o credenciales de acceso, etc. en este proyecto nos enfocaremos sobre los ataques informáticos del tipo Ingeniería social.

Como ya lo definimos previamente, la ingeniería social se basan en la manipulación de personas, con el objetivo de conseguir una meta, esta meta pueden ser, entre muchas, información confidencial, credenciales de acceso, cuentas bancarias o permisos especiales.

## 4.5 Árbol de decisiones de un atacante

De acuerdo con Bruce Schneier según la teoría de árbol de ataque comenta que esta metodología de ataques informáticos se divide en[35]:

- Nodo principal es el objetivo principal para los ataques
- Nodos hijos son los métodos para alcanzar el objetivo del nodo principal

Se pretende realizar una guia de ataque comúnmente utilizado para la realización una ataque informático, en este se detallan los pasos previos a la realización de un ataque, la información necesaria y factores claves (humanos y técnicos) involucrados en el proceso.

Para este trabajo nos incumbe el árbol de ataque utilizando en la realización de ataques de ingeniería social.

Como lo mencionamos anteriormente, la metodología mayormente utilizada para la realización de ataques de ingeniería social, consta de cuatro pasos fundamentales:

- Investigar el objetivo: Esta fase como su nombre lo indica, consiste en la búsqueda de información del objetivo. Para esta etapa se pueden realizar actividades como: búsqueda en la web del objetivo, revisión de basuras, redes sociales o incluso

[35] https://www.schneier.com/paper-attacktrees-ddj-ft.html

algunas más técnicas como escaneo de información a las páginas web de la compañía. Actualmente se encuentran adicionalmente herramientas de fácil utilización que generan la mayor cantidad de información a partir de una página web. herramientas como Basket o dradis

- Selección de la víctima: basados en la información obtenida en la etapa anterior, se procede a seleccionar el eslabón más débil de la compañía o aquella persona que tiene la información u objetivo que estamos buscando
- Establecer relación: se establece una conexión con la víctima, puede ser una llamada telefónica, un correo, entre otros
- Explotar la relación establecida: Aprovechar la conexión establecida y cumplir con la finalidad del ataque.

Es importante tener estos cuatro aspectos fundamentales en los ataques al momento de definir la estrategia de defensa a implementar en las organizaciones con el objetivo mitigar la fuga de información. Mientras menos información de la organización y sus colaboradores tengan los atacantes, menor será la probabilidad de éxito del ataque.

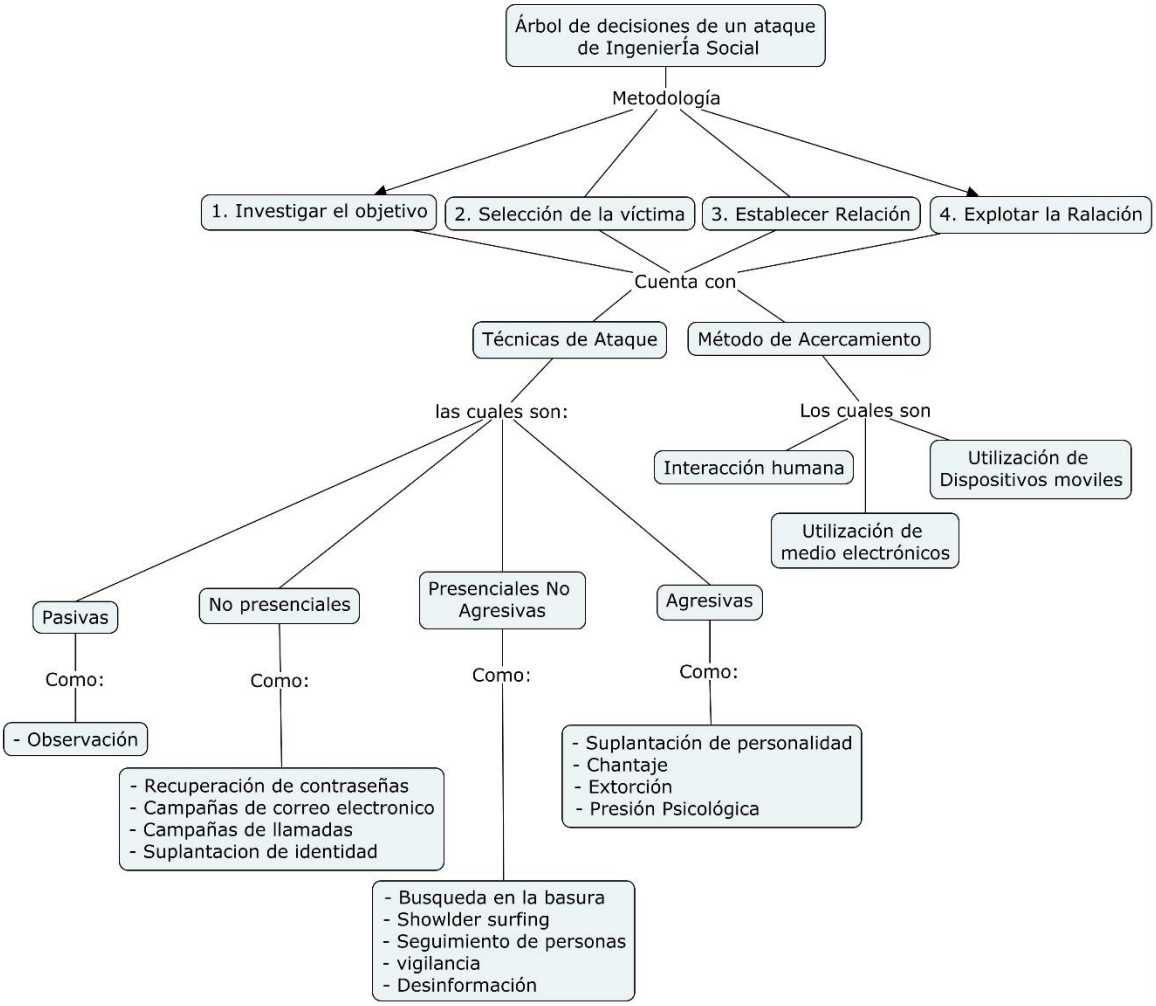



*Figura 3.* Arbol de decisiones aportes framework Ingenieria social.

## 4.6 Defensa en profundidad

La definición como tal de la oración "Defensa en profundidad", tienen sus orígenes en el ámbito militar, con el desarrollo de nuevas armas de destrucción, capaces de destruir las principales defensas de cualquier ejército, se comenzó a utilizar un tipo defensa donde se contaba con varios anillos de seguridad para proteger al líder o cualquier tipo de información confidencial o secreto militar que no querían que cayera bajo mando enemigo. Este tipo de defensa, está regido por 4 características que aseguran el correcto funcionamiento de la defensa:

- El Líder o bien que se quiere proteger, se debe encontrar en el centro de todas las líneas o capas de defensa planeadas.
- Cada una de las capas de defensa tiene un papel fundamental en la defensa global del líder o del bien
- Las líneas de defensa son autónomas, esto con el objetivo de no depender de otra capa para su funcionamiento. De esta forma si una de las capas cae, las otras no se verán afectadas.
- Cada Línea de defensa cuenta con recursos independientes para mantener la defensa.

La estrategia definida por los militares fue utilizada posteriormente en diferentes ámbitos como el nuclear, donde se utilizó para el enfriamiento de los reactores nucleares, donde se tenían diferentes estrategias para mitigar la falla del método de enfriamiento principal[36].

En el ámbito de la seguridad informática, el concepto es utilizado sin variar en su estructura principal donde la definición dada por los militares, es decir, se utilizan varias capas o líneas de defensa para la protección de la información, y en caso de que una falle, las otras se encuentran activas, aplica.

La definición de "Defensa en profundidad" dada por la SANS, Instituto especializado en la seguridad de la información y en ciberseguridad, no difiere a lo mencionado anteriormente, según ellos, la Defensa en profundidad es "La defensa en profundidad es el concepto de protección de una red de ordenadores con una serie de mecanismos de defensa, de forma secuencial, de tal forma que si un mecanismo de falla, otro que ya estarán en lugar de frustrar un ataque"[37].

El enfoque de defensa en profundidad que recomendamos en este trabajo, está centrado en la protección de la información, con tres capas principales: Personas, Tecnología y operaciones. Donde se pretende asegurar cada una de estas capas con diferentes métodos que protejan la información confidencial de la compañía[38].

---

[36]http://www.ssi.gouv.fr/archive/es/confianza/documents/methods/mementodep-V1.1_es.pdf

[37] https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525

[38] https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

- Personas: El riesgo de fuga de información clave por parte de los empleados de la compañía puede ser mitigada con la implementación de mecanismos que aseguren el adecuado trato de la información y concienticen a los empleados del valor de la información y los riesgos actuales de fuga de la misma. Algunos mecanismos son:

  - Políticas y procedimientos de seguridad
  - Campañas de entrenamiento
  - Campañas de sensibilización

- Tecnologías: Actualmente encontramos en el mercado muchas oportunidades de inversión en diferentes tipos de tecnologías o sistemas de información para nuestras organizaciones, algunas con mayores ventajas que otras y un rango de precios muy diferentes. La selección de los sistemas de información en las compañías es fundamental para el correcto funcionamiento y se busca siempre tener un balance entre calidad y precio. Es importante siempre tener en cuenta, en el momento de la adquisición de una nueva tecnología o actualización de una existente, que esta cuente con:

  - Actualizaciones periódicas de seguridad
  - Soporte a usuarios
  - Que permita la definición políticas de seguridad

También es recomendable, investigar por la reputación del sistema de información a adquirir y conocer la calificación dada por terceras partes y expertos.

- Operaciones: Consiste en mantener un correcto funcionamiento de las actividades realizadas en las organizaciones día a día. Para asegurar esto, se implementan en las organizaciones diferentes métodos como pueden ser:

  - Control de cambios en los sistemas de información
  - Actualizaciones de seguridad
  - Monitoreo constante del tráfico de red
  - Recuperación de datos (copias de seguridad)
  - Monitoreo de ataques de seguridad informática.

Con estos tres enfoques, y enfocados en los ataques de ingeniería social, pretendemos brindar a las PYMES un marco de referencia que permita asegurar su infraestructura, contra este tipos de ataque[39].

### 4.7 Planes de acción

Llamamos a los planes de acción, la guía que nos permite reaccionar a los diferentes tipos de ataques de ingeniería social que presenten nuestras organizaciones. Dichos planes de acción estarán enfocados en los diferentes procedimientos a efectuar de acuerdo a un marco de referencia el cual estará descrito más adelante en este mismo documento. Los planes de acción estarán divididos en dos. Planes de acción preventivos y planes de acción correctivos.

- Planes de acción preventivos: Son aquellos mecanismos implementados para prevenir un ataque informático. Estos planes de acción deben ser implementados y mantenidos en el tiempo ya que son la primera capa de defensa implementado en nuestra organización.
- Planes de acción correctivos: Son mecanismos implementados una vez la compañía sea o se encuentre bajo ataque. estos mecanismos pretenden identificar el daño efectuado por los atacantes y el cierre de entradas traseras configuradas por el atacante así como la recuperación de información y lecciones aprendidas.

Los planes de acción, estarán descritos como una respuesta frente a los diferentes pasos realizados por los atacantes para efectuar un ataque de ingeniería social, donde cada uno de los pasos o árbol de decisión del atacante estará cubierto con un plan de acción o mecanismos implementados para prevenir la intrusión.

### 4.8 Evaluación de riesgos y Vulnerabilidades

Para la evaluación de riegos debemos de suponer que la compañía está expuesta a ataques (Metodología inversa donde se plantea que tipo de eventos se pueden presentar), en donde se deben de identificar los elementos principales para la administración de seguridad, y categorizar y priorizar los riesgos según los proceso, esta categorización puede ser:

- Información confidencial

[39] https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

- Recursos
- Dinero

Esta clasificación se realiza dependiendo del Core del negocio de las organizaciones, y para esto nos podemos basar en el ciclo de vida PHVA en donde debemos de especificar:

- Identificación de inventario de activos de información y clasificación según los procesos de la compañía, teniendo en cuenta la información que es confidencial y debe protegerse.

- Identificar las vulnerabilidades y amenazas de cada uno de esos activos de información identificados en la fase anterior, con el fin de buscar un plan de acción para sensibilizar a los usuarios de los posibles riesgos que se pueden materializar si hay una fuga de información

- Comunicarles a los propietarios cada uno de los activos comunicado la información de los cuales son responsables para que se asignen las responsabilidades a las personas adecuadas.

- Comunicar a cada uno de los usuarios responsables de esos activos de información el impacto que representa perdida de información en cuanto a confidencialidad, integridad y disponibilidad.

- Diseñar planes de acción para sensibilizar a los usuarios en cuanto a seguridad de la información, para esto definir políticas de seguridad, definir una matriz de roles y responsabilidades. esto con el fin de crear campañas para formar una cultura en seguridad de la información[40].

Para la evaluación de riesgos proponemos realizar un mapa de riesgos en el cual se puede especificar la siguiente información:

- Detalle del riesgo
- Descripción

[40] http://apuntesdeinvestigacion.upbbga.edu.co/wp-content/uploads/ESI-Luis-Eduardo-Pati%C3%B1o-Dur%C3%A1n.pdf

- Causa
- Efecto
- Clasificación
- Análisis (Calificación y Evaluación)
- Valoración (Probabilidad e impacto)
- Definición de políticas para la mitigación de los riesgos.

Según la definición que se tenga de la evaluación de riesgos en el mapa que se construya se puede tener en cuenta una columna donde se especifique la vulnerabilidad que tiene cada uno de esos riesgos, esto con el fin de realiza un plan de acción para que no se materialicen los riesgos.

# 5 Aporte framework ingeniería social

Es un diseño o una estrategia reutilizable, la cual se utiliza como guía en la ejecución o implementación de un proyecto. El framework, nos brindará información sobre alguna actividad que deseamos ejecutar, como la ejecutamos, y los posibles resultados que obtendremos.

Enfocado en el trabajo actual, el framework que desarrollaremos permitirá a una compañía, evaluar el nivel de riesgo al que se encuentra expuesto la información que se considere como crítica e implementar mecanismos para proteger dicha información.

El framework o marco de trabajo que se presentará a continuación, está enfocado en las los 4 pasos utilizados por un atacante para la realización de ataques de ingeniería social descritos anteriormente, y recomendará estrategias para minimizar la exposición protección de información.

## 5.1.1 Calificación del valor de información

En la implementación de una estrategia de seguridad que proteja la información confidencial de la compañía contra ataques de tipo de ingeniería social, es importante inicialmente definir, qué información desea proteger.

Este aspecto es fundamental ya que la implementación de mecanismos de protección, puede llegar a tener altos costos de inversión tanto de dinero como de tiempo, y es por esto que no debemos proteger aquello que no nos es de alta importancia. No es lo mismo, en

cuanto al valor de la información, que se filtren los estados financieros de la compañía, si lo comparamos con la pérdida de un correo electrónico con una solicitud de un producto.

Para poder definir qué información es crítica, debemos, inicialmente conocer, las características principales de la información.

- Confidencialidad: Cuando hablamos de confidencialidad de la información, nos referimos a aquellas personas, o sistemas que tienen acceso. La información, solo debe ser conocida por aquellos medios que la requieran para cumplir con un objetivo específico y que se encuentre autorizado para tenerla. decimos que la confidencialidad de la información fue vulnerada, cuando una entidad, obtiene información sin estar autorizado o que no la requiere para sus proceso. un ejemplo en la fuga de información confidencial de la información, fue el famoso caso de wikileaks, donde sin previa autorización fueron publicados documentos sensibles del ejército y el departamento de defensa de los Estados unidos de Norte America. Se puede conocer más sobre este caso en el enlace a continuación[41].

- Integridad: La integridad se refiere a que la información que tenemos es la que requerimos al momento de realizar una actividad y que esta no fue modificada por personal o sistemas no autorizados. Decimos que la integridad de la información fue violada cuando esta es modificada por un externo ajeno a un proceso para obtener un beneficio o perjudicar a alguien más.

- Disponibilidad: Esta característica permite que la información que se requiere esté disponible en el momento en el que es requerida por un sistema o persona para cumplir con sus funciones. Los ataques a la disponibilidad de la información, o mejor conocidos como ataque de denegación de servicios, es actualmente el ataque preferido por los diferentes grupos de hacktivistas. Donde por medio de la solicitud masiva de servicios a una página o servicio, colapsa debido al alto flujo de información transmitida.

### 5.1.2 Selección de información crítica

[41] http://www.bbc.com/mundo/internacional/2010/04/100406_2317_wikileaks_sitio_gz.shtml

La selección de la información crítica, es simple una vez conocemos las características de la información. Para la selección debemos preguntarnos, qué pasaría si la información evaluada no está disponible, si no tiene integridad o si la información se filtra.

Podemos evaluar el impacto de la pérdida de cualquiera de las tres características, pensando en una afectación para los procesos como económicos para la organización calificando por ejemplo de 1 como bajo, a 5 como muy alto, la vulnerabilidad de cualquiera de las 3 características mencionadas.

Posteriormente sacaremos un promedio de la calificación dada a cada activo de información sumando la evaluación de los impactos y dividiendo por las 3 características. Los activos de información con un promedio mayor, serán los que calificamos como información crítica. Otra forma para calificar la información crítica es determinar un promedio base. Todo lo que está sobre el promedio base, será catalogado como crítico, y lo que esté por debajo será información no crítica.

Para comprender esta estrategia, realizaremos un ejemplo ficticio de un proceso comúnmente utilizado en las organizaciones. El pago a proveedores.

Para realizar el pago a proveedores requerimos, entre otros, la siguiente información:

- Valor del producto adquirido o servicio solicitado
- Datos de la cuenta bancaria
- Datos del portal bancario para realizar el pago
- Descripción del servicio prestado

Ahora, realizamos la métrica preguntando qué impacto tendría para la organización la violación de las 3 características:

| Cual seria el impacto si pierdo la: | Integridad | Disponibilidad | Confidencialidad |
|---|---|---|---|
| Valor del producto adquirido o servicio solicitado | 5 | 3 | 3 |
| Datos de la cuenta bancaria del proveedor | 3 | 1 | 2 |
| Datos del portal bancario para realizar el pago | 3 | 3.5 | 5 |
| Descripción del servicio prestado | 1 | 2 | 2 |

*Figura 4.* Métrica de impacto.

Una vez realizado la calificación, procedemos a realizar el promedio teniendo como base la calificación de 3.5

| Cual seria el impacto si pierdo la: | Integridad | Disponibilidad | Confidencialidad | Promedio |
|---|---|---|---|---|
| Valor del producto adquirido o servicio solicitado | 5 | 3 | 3 | 3.6666667 |
| Datos de la cuenta bancaria del proveedor | 3 | 1 | 2 | 2 |
| Datos del portal bancario para realizar el pago | 3 | 3.5 | 5 | 3.8333333 |
| Descripción del servicio prestado | 1 | 2 | 2 | 1.6666667 |

*Figura 5.* Calificación de impactos.

Como resultado, tendríamos que en el proceso de pago a proveedores para nuestros ejemplo, la información crítica seria: El valor de producto adquirido o servicio prestado y los datos del portal bancario para realizar el pago.
Sobre estos resultados, procederíamos a la evaluación de los riesgos de ataques de ingenieria social presentados en Framework desarrollo en este trabjo, adicionalmente la implementación de controles que impidan la violación de cualquiera de las 3 características de la información.

### 5.1.3 Estructura marco de trabajo (Framework)

Realizamos la siguiente estructura de marco de referencia para el aporte al framework respecto identificación, prevención y mitigación de los ataques a través de ingeniería social, marco cuenta con:

- *Técnica*: presentamos los tipos de técnicas de ataques sobre los cuales vamos hacer el análisis de tipos de ataques, vulnerabilidad y acciones correctivas.

- *Método de acercamiento*: Definimos como va hacer la interacción con la víctima o persona a la cual se realizara ingeniería social (Interacción humana, PC o movil).

- *Nombre de ataque*: Nombre denominado para el ataque.

- *Fase del árbol de decisiones:* Se aplica la metodología para identificar en qué momento se deben de ejecutar los ataques, estos son:

  - Investigar el objetivo
  - Selección de la victima
  - Establecer relación
  - Explotar la relación establecida.

- *Descripción del ataque:* Se define el tipo de ataque se va a realizar.

- *Evaluación de la vulnerabilidad enfocada en el ataque:* presentamos el análisis de vulnerabilidad en cuanto al ataque se va a realizar.

- *Acción correctiva de la vulnerabilidad:* Análisis del método que sebe debe de seguir para mitigar que el riesgo asociado a la vulnerabilidad se materialice.

### 5.1.4 Marco de trabajo (Framework)

| Técnica | Método Acercamiento | Nombre de Ataque | Fase en el árbol de decisiones | Descripción del ataque | Evaluación de vulnerabilidad | Acción correctiva |
|---|---|---|---|---|---|---|
| Pasiva | Interacción Humana | Uiltización investgación del objetivo<br><br>Registros DNS<br><br>Whois<br><br>Osint | • Investigar el objetivo<br>• Selección de la victima | Este metodo permite a un atacante obtener información como propietario de un dominio o una dirección IP, nombres de servidores, paginas, subdomino, servidores de correo electronico, bases de datos y metadata.<br><br>Este metodo de investigacion no involucra la participacion de la victima y se basa en información disponible publicamente. | Realizar consultas por medio de herrameintas informaticas sobre información publica compañía, esta herramientas pueden ser:<br><br>• Foca<br>• Whois<br>• Maltego<br><br>Una vez identificada la información publica realizar una análsis de la criticidad e impacto recomendada en este trabajo, con el objetivo de cuantificar la vulnerabilidad y exposición de la información critica de la compañía. | Identificar por medio de la herramientas utilizadas en la evaluación de la vulnerabilidad los puntos de fuga de la información critica de la compañía, una vez identificados los puntos de fuga eliminar el contenido publico o exposicion de la red los documentos conciderados como información critica.<br><br>Realiza una nueva consulta con el objetivo de asegurar que no se encuentra expuesta la información identificada anteriormente. |
| Activa | Interacción Humana | Investigación del objetivo. | • Investigar el objetivo<br>• Selección de la victima | Como su nombre lo indica, este método permite a un atacante obtener información básica | Para evaluar la vulnerabilidad de la compañía frente a este tipo de ataque, se debe inicialmente seleccionar una muestra de empleados cuyos cargos epongan las información | Definir para las áreas o puntos de contacto de la organización (Perimetro) con personal externo, una politicas y procedimiento donde se definan la información que puede suminitrar, este procedimiento debe ser |

| Técnica | Método Acercamiento | Nombre de Ataque | Fase en el árbol de decisiones | Descripción del ataque | Evaluación de vulnerabilidad | Acción correctiva |
|---|---|---|---|---|---|---|
| | | | | requerida para la realización de un ataque de ingeniería social. Datos como: dirección, teléfonos, personal de contacto. | clasificada como critica de acuerdo con la tecnica de clasificación de información descrita recomendada en este documentos.<br><br>Sobre esta muestra se deben realizar tecnicas de obtención de informacion (Nombres, correos, direcciones, horarios de atencion, puntos de contacto, ubicación de áreas) como:<br><br>• Llamanda telefonica.<br>• Correo electronico.<br>• Consulta pagina Web.<br><br>Aunque esta información, puede no estar catalogada como confidencial, para un atacante puede ser fundamental, ya que permite entre otros, seleccionar las victimas de ataque, horarios para la realización de ataques o puntos de acceso para vulnerar la seguridad de la compañía. | socializado al momento de realizar el ingreso de empleados y debe contar con la firma del empleado donde certifique que entiende el procediendo o política.<br><br>Como ejemplo se puede desarrollar un guion para el empleado que atiende las llamadas para prestar atención a las solicitudes o requerimientos realizados, Esto con el objetivo de establecer una temática en la conversación realizada, y cualquier cambio sea rechazado por el empleado |

| Técnica | Método Acercamiento | Nombre de Ataque | Fase en el árbol de decisiones | Descripción del ataque | Evaluación de vulnerabilidad | Acción correctiva |
|---|---|---|---|---|---|---|
| | | | | | Si bien la entrega de información básica no representa un peligro, es importante conocer el tipo de información que se está entregando a los externos de la organización con el objetivo de restringir aquella que no es fundamental para la consecución de un proceso. | |
| Activa no presenciales | Interacción Humana | Phishing Telefónico | • Establecer relación<br>• Explotar la relación | El phishing es una técnica en la cual el atacante se hace pasar por un ente de confianza con el objetivo de obtener información confidencial. En el phising telefónico se suplanta personal con aparente autorización para la solicitud de información como puede ser: personal del área de TI de las organizaciones, Jefes de otras áreas, proveedores o | Para la evaluación de la vulnerabilidad a este tipo de ataque es la realización del ataque en si a un número previamente definido de empleados seleccionados aleatoriamente. Para la realización del ataque se recomienda el siguiente procedimiento ***Ver anexo 1 – Ataque phising llamada telefonica***<br><br>Este ataque debe ser realizado por personal interno de la organización o un tercero con el debido modelo de hacking etíco y con autorización de la alta gerencia, ya que se manejará información | Para minimizar la vulnerabildiad asociada a este tipo de ataques, se utilizarán las siguientes actividades<br><br>a- Realizar campañas frecuentes de concientización dirigidas a los empleados de la compañía, con el fin de recalcar la importancia no suministrar ningún tipo de información vía electronica a desconocidos. Estas campañas pueden ser:<br><br>• Correo electrónicos<br>• Publicidad<br>• Panfletos<br><br>b- Realizar un documento formal donde se recalque la importancia de no suministrar información vía electronica a personas desconocido, este |

| Técnica | Método Acercamiento | Nombre de Ataque | Fase en el árbol de decisiones | Descripción del ataque | Evaluación de vulnerabilidad | Acción correctiva |
|---|---|---|---|---|---|---|
| | | | | consultores, entre otros | confidencial de los empleados como contraseñas de acceso a los sistemas de información.<br><br>Luego de realizada la prueba, se recomienda comunicar por cualquiere medio el ataque a la organización informando la realización de la misma y el objetivo de la prueba con el fin de aclarar cualquier alerta generada en la organización y la modificación de las contraseñas obtenidas en la realización de las pruebas | documento deberá ser leído y firmado por cada empleado al momento de ingresar a nuestras organizaciones<br><br>Es importante aclarar que los empleados, son el eslabón más vulnerable, y que esta brecha no podrá ser mitigada en su totalidad, sin embargo, el conocimiento y la importancia de la no divulgación de las credenciales de acceso y las campañas constantes mitigan en una proporción importante la vulnerabilidad. |
| | Medios electronicos | Correo Electronico Phising | • Establecer Relación<br>• Explotar la relación | El phishing es una técnica en la cual el atacante se hace pasar por un ente de confianza con el objetivo de obtener información confidencial. El Phishing por correo electrónico se refiere a la | Un método que permite evaluar la vulnerabilidad de las organizaciones frente a este tipo de ataques, requiere la realización del ataque en sí. Para la realización del ataque y la medición de los resultados, a continuación, se adjunta el procedimiento para la implementación de la prueba. Este ataque | Para minimizar la vulnerabildiad asociada a este tipo de ataques, se utilizarán las actividades que brindaran a los empleados conciencia sobre el cuidado he importancia de las credenciales de acceso a nuestros sistemas:<br><br>a- Se recomienda realizar campañas frecuentes de concientización dirigidas a los empleados de la compañía, con el fin de |

| Técnica | Método Acercamiento | Nombre de Ataque | Fase en el árbol de decisiones | Descripción del ataque | Evaluación de vulnerabilidad | Acción correctiva |
|---|---|---|---|---|---|---|
| | | | | técnica de envió de un link por medio de un correo electrónico, con un remitente aparentemente autorizado, a una página web, la cual simula ser una página de confianza. El correo se envía con el objetivo de obtener la información diligenciada en las páginas suplantadas. | debe ser realizado por personal interno de la organización o terceros en compañía de TI y con autorización de la alta gerencia, ya que se manejará información confidencial de los empleados como contraseñas de acceso a los sistemas de información, el procedimiento de ataque recomendado se puede observar en: ***Ver anexo 2 – Ataque correo electronico Phising***<br><br>Luego de realizada la prueba, se recomienda enviar un correo electrónico a la organización informando la realización de la misma y el objetivo de la prueba con el fin de aclarar cualquier alerta generada en la organización y la modificación de las contraseñas obtenidas en la realización de las pruebas<br><br>Nota: El método presentado, permite la obtención de nombres de usuario y contraseñas de acceso | recalcar la importancia no suministrar ningún tipo de información vía correo electrónico a desconocido. Estas campañas pueden ser:<br><br>• Correos electrónicos<br>• Publicidad<br>• Panfletos<br>• eventos<br><br>b - Realizar un documento formal donde se recalque la importancia de no suministrar información vía correo electrónico a desconocidos, este documento deberá ser leído y firmado por cada empleado al momento de ingresar a nuestras organizaciones.<br><br>Por parte de los administradores de sistemas, es importante contar con un procedimiento de finido para la instalación de parches de seguridad suministrado por los proveedores de los sistemas operativos y bases de datos, ya que estas, cuentan con técnicas de identificación de ataques tipo phising.<br><br>Dictar charlar o cursos a los empleados, con el objetivo de enseñar a identificar correos o ataques tipo |

| Técnica | Método Acercamiento | Nombre de Ataque | Fase en el árbol de decisiones | Descripción del ataque | Evaluación de vulnerabilidad | Acción correctiva |
|---|---|---|---|---|---|---|
| | | | | | a la red de las compañías, pero puede, en cualquier caso, ser modificado para obtener cualquier otro tipo de información. | phishing a los empleados, este curso debe contar con las siguientes secciones:<br>• Identificación de correos phishing.<br>• Verificar fuente de información de los correos.<br>• No ingresar a paginas web por medio de Hipervinculos.<br>• Ante la duda informar al area de seguridad.<br>• Modificación periodica de contraseñas. |
| | | Baiting | Explotar la relación | Esta técnica consiste en dejar un medio de almacenamiento externo como USB, cd o discos duros, en lugares con alto flujo de personal de la organización que se desea atacar, con el objetivo de transmitir virus o malware al momento de conectar el medio en las máquina de los empleados | Para la realización de esta prueba, se debe realizar una visita a los diferentes puestos de trabajo con el objetivo de identificar las políticas configuradas en las maquinas en cuanto a :<br>• Configuración del autor run (auto ejecutar)<br>• Lecutra de CD´s<br>• Lectura de USB y discos duros externos<br>Con esta información, evaluar la necesidad de tener activos | Para la corrección de esta brecha de seguridad se recomienda la realización de los siguientes dos procedimientos:<br>• Deshabilitar el auto-run<br>• Deshabilitar unidad de CD:<br>• Deshabilitar lectura de USB y medios extraíbles<br>Adicionalmente se recomienda la instalación de antivirus y anti – malwares, en las maquinas de las compañias y asegurara que estas se encuentran actualizadas. |

| Técnica | Método Acercamiento | Nombre de Ataque | Fase en el árbol de decisiones | Descripción del ataque | Evaluación de vulnerabilidad | Acción correctiva |
|---|---|---|---|---|---|---|
| | | | | | dichos componentes y deshabilitar en las máquinas de los usuarios que no requieran las funcionalidades. | |
| Activas Presenciales no agresiva | Interacción Humana | Búsqueda en la basura (Dumpster Diving) | Investigar el objetivo | Como su nombre lo indica, esta técnica permite la consecución de información por medio de la búsqueda de las desechos (documentación eliminada física o tecnologica, recostrucción de información de maquina obsoletas) de la organizaciones. | Para la identificación de la vulnerabilidad frente a este ataque, se debe conocer el manejo de las deposiciones o renovaciones de la organización.<br><br>¿Dónde se almacenan los documentos eliminados por los empleados?<br><br>¿Son destruidos los documentos en las desechados de los empleados?<br><br>¿Quién manipula los desechos de la organización?<br><br>¿Se cuenta con procedimiento de destrucción de documentación sensibles, para la organización?<br><br>¿Se cuenta un procedimietno para la eliminación de información almacenada en computarodres o | Para la mitigación de este riesgo, es importante definir e implementar procedimientos de destrucción de documentación, así como la limitación de accesos a las áreas donde son almacenadas los desechos de la compañía asegurando que ningún documento de la pueda ser revisado por personal ajeno.<br><br>Adicionalmente realizar un analisis en las maquinas obsoletas que vayan a ser donadas que no se encuentren información confidencial, la cual no pueda ser obtenida por tecnicas de análisis forence. |

| Técnica | Método Acercamiento | Nombre de Ataque | Fase en el árbol de decisiones | Descripción del ataque | Evaluación de vulnerabilidad | Acción correctiva |
|---|---|---|---|---|---|---|
| | | | | | servidores obsoletos en la compañía previo a su destrucción o donación?<br><br>Aunque a simple vista la evolución de este riesgo no parece importante, en las deposiciones de nuestra organización pueden estar almacenados datos como: Estados financieros, información confidencial de los empleados, contrato con compañías asociadas, entre muchos | |
| | | Mirar por encima del hombro (Shoulder surfing) | Investigar el objetivo | Esta técnica se refiere al acto de recaudar información por medio de la observación. Es comúnmente utilizada para obtener credenciales de acceso buscando en los puestos de trabajo de los empleados en las notas (post-it) | Para la evaluación de este riesgo, Inicialmente se debe realizar una muestra aleatoria de trabajadores de la organización para posteriormente realizar una visita sorpresiva a los puestos de trabajo, donde debemos buscar toda aquella información que este a la vista de cualquier persona y pueda ser catalogada como confidencial. | Se deben realizar campañas de seguridad por correo electrónico, panfletos y comunicación interna donde se defina la importancia de la información confidencial y de no escribir contraseñas en papeles a la vista de todo el mundo.<br><br>Adicionalmente incluir en la política de seguridad de la compañía, la no escritura de contraseñas de seguridad o información confidencial en notas visibles o almacenadas con poca seguridad |

| Técnica | Método Acercamiento | Nombre de Ataque | Fase en el árbol de decisiones | Descripción del ataque | Evaluación de vulnerabilidad | Acción correctiva |
|---|---|---|---|---|---|---|
| | | | | dejadas en las pantallas o debajo de los teclados de los empleados, entre otros. | Los resultados de las visitas deben ser diligenciados y cuantificados dependiendo del porcentaje de hallazgos de la siguiente forma:<br><br>Se realizará una comparación entre la cantidad de empleados sobre los cuales se encontraron información confidencial y la totalidad de visitas realizadas con el objetivo de determinar el porcentaje de éxito de la prueba. Para esto se realizará la siguiente operación matemática:<br><br>$\left(\frac{a}{b}\right) * 100$<br><br>Donde:<br><br>a - será la cantidad de usuarios que suministraron las credenciales de acceso<br>b - será la cantidad de usuarios a los que se les envió el correo<br><br>Dependiendo de los resultados obtenido por la operación matemática se podrá evidenciar que tan fuerte o débil esta la concientización de usuarios respecto | |

| Técnica | Método Acercamiento | Nombre de Ataque | Fase en el árbol de decisiones | Descripción del ataque | Evaluación de vulnerabilidad | Acción correctiva |
|---|---|---|---|---|---|---|
| | | | | | escribir sus contraseñas o información confidencial. | |
| Activa agresivas | Interacción Humana | Seguir de Cerca (Tailgating) | Explotar la relación | Esta técnica se refiere al acto de ingresar a áreas restringidas de una organización, siguiendo a personal autorizado de cerca. Por ejemplo cuando un empleado abre una puerta con acceso electrónico y no verifica el cierre de la misma, y otra persona aprovecha para ingresar. | Para la realización de esta prueba de vulnerabilidad, se requiere la participación de personal externo a la organización. El objetivo de esta persona es tratar de ingresar a lugares restringidos de la organización, sin ser detectado ni poseer ningún tipo de autorización.<br>En caso de que el externo logre ingresar sin problemas a las diferentes áreas, evaluar la posibilidad de implementar los mecanismos mencionados en la acción correctiva. | Para mitigar el riesgo asociado a este riesgo, se debe implementar y socializar unos procedimientos, el cual obligue a la totalidad de empleados a portar el carnet de empleados siempre visible.<br>Para los visitantes, se debe exigir el registro en la recepción de la organización y la entrega de un carnet con la palabra "visitante" escrita en él.. Este registro, debe estar, para todos los casos, soportado por alguna persona autorizada al interior de la organización. No se permite el ingreso de personal externo sin una reunión o autorización previa. Dicho carnet también debe estar en lugar siempre visible.<br><br>El procedimiento además debe incluir un párrafo donde se especifique que el tránsito de personas por la organización sin carnet está restringido. |
| | | Extorciones | Explotar la relación | Esta técnica consiste en obligar a la víctima a entregar la | Si bien no podemos probar la capacidad de nuestros empleados para resistir la | Es importante que a la hora de definir las responsabilidades de un cargo, se defina el alance de |

| Técnica | Método Acercamiento | Nombre de Ataque | Fase en el árbol de decisiones | Descripción del ataque | Evaluación de vulnerabilidad | Acción correctiva |
|---|---|---|---|---|---|---|
| | | | | información deseado por medio de violencia o intimidación. | intimidación frente a solicitudes de información violenta, si podemos implementar mecanismos que impidan que la información en su totalidad sea entregada. Ver acciones correctivas. | la información que este debe tener.<br>Siempre debemos tener presente en a la hora de crear un cargo, que dicho cargo no cuente con facultades para la realización de un proceso completo. Un ejemplo de lo que no se puede hacer, sería el de un tesorero con facultades para realizar la solicitud de compra de un artículo, la aprobación de compra del articulo y la transferencia de fondos para la compra. Si segregamos la actividad mencionada (compra de un artículo), en dos personas distintas, el proceso no podría ser completado sin la participación de las dos, y en el caso de un atacante, que extorción a uno de los empleados, no lograría su objetivo ya que el solo no tendría permisos para completar el proceso.<br><br>Es por esto que siempre debemos segregar las funciones o actividades de la compañía, para evitar este tipo de fraudes. |
| | | Conseguir trabajo en la victima | • Establecer Relación<br>• Explotar la relación | Esta técnica consiste en conseguir trabajo en pequeñas y medianas empresas, | Evaluar el proceso de selección aplicado en la compañía, verificando que el procedimiento cuente con: | Definir e implementar un procedimiento para la contratación de empleado, el cual obligue a la realización de las siguientes actividades: |

| Técnica | Método Acercamiento | Nombre de Ataque | Fase en el árbol de decisiones | Descripción del ataque | Evaluación de vulnerabilidad | Acción correctiva |
|---|---|---|---|---|---|---|
| | | | | donde el proceso de selección no es muy elaborado ni se investiga a los postulantes | • Verificación en centrales de riesgos.<br>• Verificación del pasado judicial<br>• Verificación de referencias personales<br>• Verificación de referencias empresariales<br>• Visita domiciliara<br>• Revisión psicológica<br><br>En caso de identificar falla en cualquiera de los puntos del procedimiento mencionado, ver acciones correctivas. | • Verificación en centrales de riesgos.<br>• Verificación del pasado judicial<br>• Verificación de referencias personales<br>• Verificación de referencias empresariales<br>• Visita domiciliara<br>• Revisión psicológica<br><br>En caso de que un empleado prospecto, no pase con la totalidad de las actividades, abstenerse de la contratación de este y continuar la búsqueda. |

# 6 Conclusiones

Actualmente las organizaciones cuentan con activos de información para los cuales se tiene una protección a través de seguridad de información desde el punto de vista tecnológico y de los procesos de la organización, ya que se cuenta con un conocimiento en cuanto a herramientas, en donde se puede realizar un análisis de los riesgos y vulnerabilidades según los procesos Core del negocio, sin embargo están dejando a un lado una de las más importantes fugas de información como lo son las personas.

Para las organizaciones debe de ser fundamental realizar estrategias de concientización a los empleados en cuanto a seguridad de la información esto a través de campañas que puedan promover una cultura organizacional de seguridad de la información y que se esté actualizando ya que la innovación de tecnologías y amenazas diariamente van evolucionando.

Nuestros aporte como estrategias de identificación, prevención y mitigación de ataques de ingeniería social al framwork sirve para disminuir la fuga de información de la organización, sin embargo debe de ir de la mano de la concientización de los empleados para que los riesgos de ataques a través de este método no se materialicen.

Es importante conocer las tecnicas y arboles decisiones en los aquetes de ingenieria social, para poder implemnetar mecanimos de seguridad que prevengan la fuga de información, si se conoce la metodologia y pasos utilizados se puede desarrollar un conjunto de procedimiento asociados a dicha metodologia.

# 7 Bibliografía

Kevin D. Mitnick, William L. Simon, (2002). The Art of Deception: Controlling the Human Element of Security

James S. Tiller, (2004). The Ethical Hack : A Framework For Business Value Penetration Testing

Donn B. Parker, (1998). Fighting Computer Crime: A New Framework for Protecting Information

J Wylder, (2003). Strategic Information Security

Amanda Andress, (2003). Surviving Security : How To Integrate People, Process, And Techno.

# 8 Anexos

## 8.1.1 Anexo 1 – Ataque Phising llamada telefonica

**Phishing telefonía.**

**Preparación del ataque phishing telefónica**
Para realizar esta prueba y con el objetivo de no improvisar ni mostrar inseguridad en las llamadas y dar una alerta a las víctimas, aconsejamos la realización de un guion que nos permita enfocar la llamada hacia los objetivos planeados, dando un parte de seguridad a la víctima de que pertenecemos a la organización y que nuestra llamada es inofensiva.

Para la creación del guion, al igual que para todas las pruebas de ingeniería social se requiere tener un conocimiento general de la empresa víctima y así estructurar el guion enfocado a nuestra víctima.

El guion deberá contar con:

- Algún proveedor de la compañía o nombre de la mesa de servicio
- Un problema ficticio sobre alguna de las aplicaciones o plataformas de la compañía
- De ser posible nombre de la víctima, en caso de no tenerlo preguntarlo en la llamada

Como ejemplo a continuación se mostrara un guion el cual podría ser utilizado para adquirir credenciales de acceso en compañías objetivos:

Buenas tardes,

*Mi nombre es **Nombre inventado*** soy Consultor de **compañía inventada*** en el proyecto implementación de **Proyecto inventado*** para nombre **empresa victima***, y actualmente estamos resolviendo unos problemas que registra tu cuenta de usuario en **Proyecto inventado***. Por favor me confirmas, tu nombre completo es ___*, tu área actual es ___* y tu cuenta de usuario es ___*. Ok, correcto, estamos viendo que se han presentado algunos intentos fallidos de acceso durante el mes pasado y tendré que modificar tu contraseña, por seguridad el sistema te solicitará cambio cuando vuelvas a ingresar, ¿cuál es tu contraseña actual? ___**

*Gracias. Disculpa, en este momento no pudimos cambiar su contraseña, por lo que continuarás usando la que tienes actualmente.*

*Le recuerdo que ante cualquier duda, por favor comunicase con soporte en TI.*

*__*Información suministrada por los funcionarios de la compañía*

**Información creada para engañar a las personas*

Como lo pudimos ver en el guion utilizado, el conocimiento de la compañía es un componente clave en el éxito de nuestra prueba. Conocer personal clave, aplicativo frecuentemente utilizado, proveedores o cualquier información que nos identifique ante los usuarios como personal inofensivo, ayudara para obtener las credenciales de acceso.

Es importante aclarar que el guion debe ser ajustado por cada prueba realizada, y crearlo basado en las necesidades y características que tenga nuestra víctima, ya sea cliente o persona.

**Resultados obtenidos del ataque phishing telefónico:**
Al igual que con la clonación de páginas web, como resultado de la realización de las pruebas de phishing por llamadas telefónicas, se obtendrá las credenciales de acceso a la página atacada de un número determinado de usuarios.

Para el análisis de la los resultados, se realizará una comparación entre la cantidad de empleados que suministraron credenciales de acceso y la totalidad de los correos enviados con el objetivo de determinar el porcentaje de éxito de la prueba. Para esto se realizará la siguiente operación matemática:

$$\left(\frac{a}{b}\right) * 100$$

Donde:

A - será la cantidad de usuarios que suministraron las credenciales de acceso
B - será la cantidad de usuarios a los que se les realizo una llamada

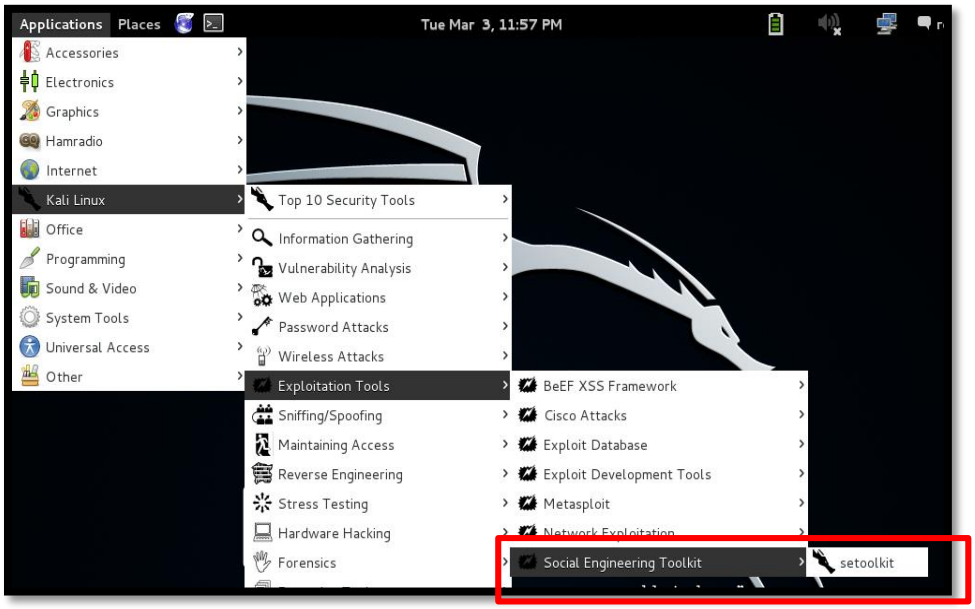
Dependiendo de los resultados obtenido por la operación matemática podremos evidenciar que tan fuerte o débil esta la concientización de usuarios respecto a divulgación de usuarios y contraseñas con el objetivo de tomar acciones correctivas.

### 8.1.2 Anexo 2 – Ataque corrego electronico Phising

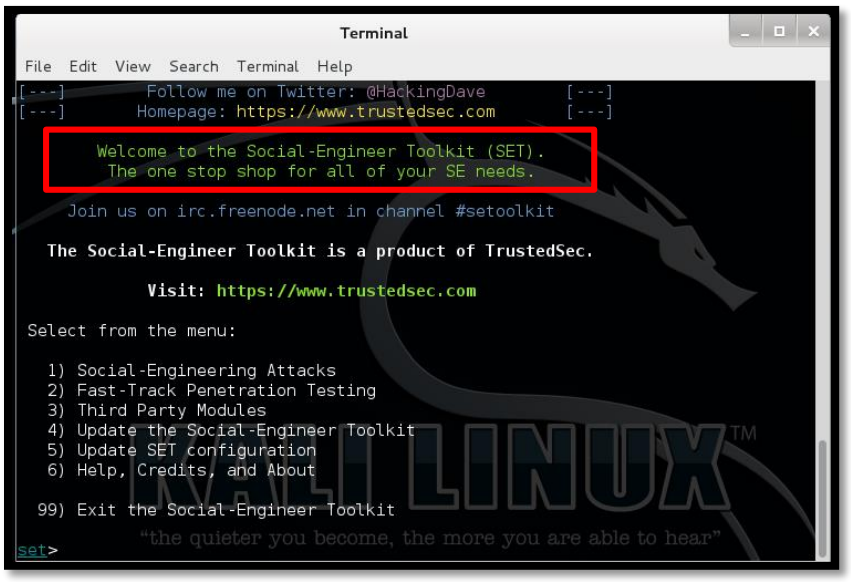
**Preparación página clon Phising**

Pantalla inicial del Kali


Para ingresar al aplicativo SET (Social engeniering Toolkit) utilizado en el ataque se ingresa por la siguiente ruta:



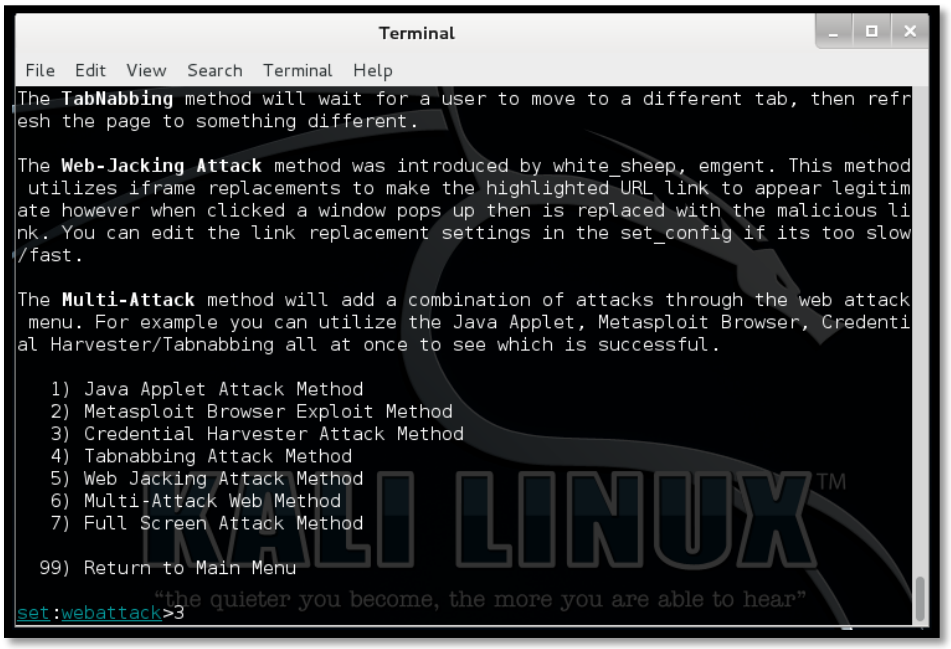

Una vez iniciado el aplicativo se inicia con la secuencia de pasos para la clonación del sitio Web seleccionado para las pruebas. A continuación se ilustra la pantalla inicial del aplicativo SET:



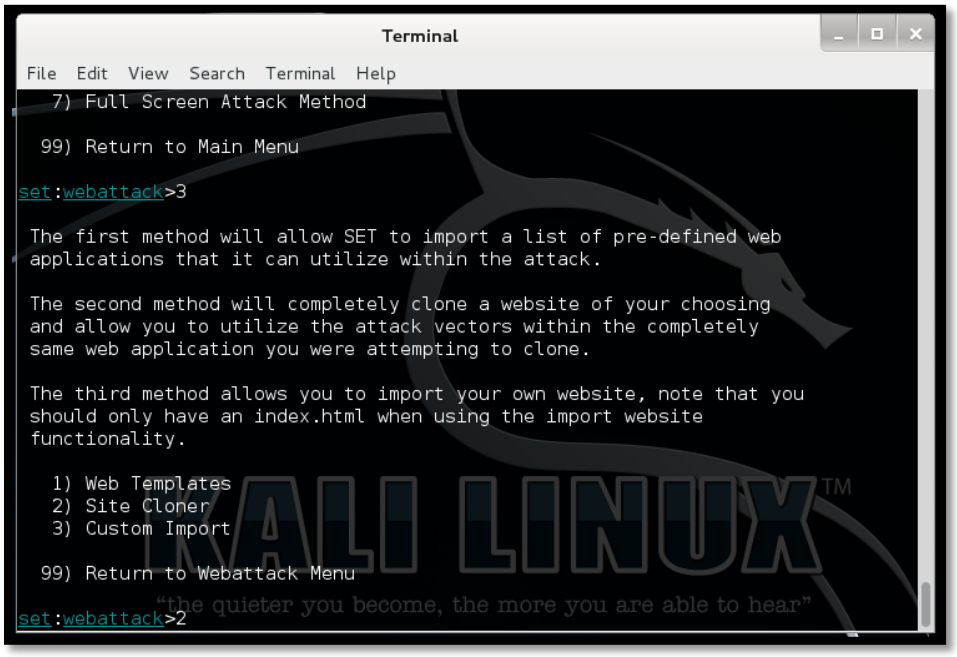

- Se selecciona la opción "1- Social Engineering attacks" del aplicativo la cual indica que se va a realizar ataques de ingeniería social


- A continuación se ingresa la opcion “2- website attack Vector”. Con esta opción se indica que va a utilizar como vector de ataque las paginas web

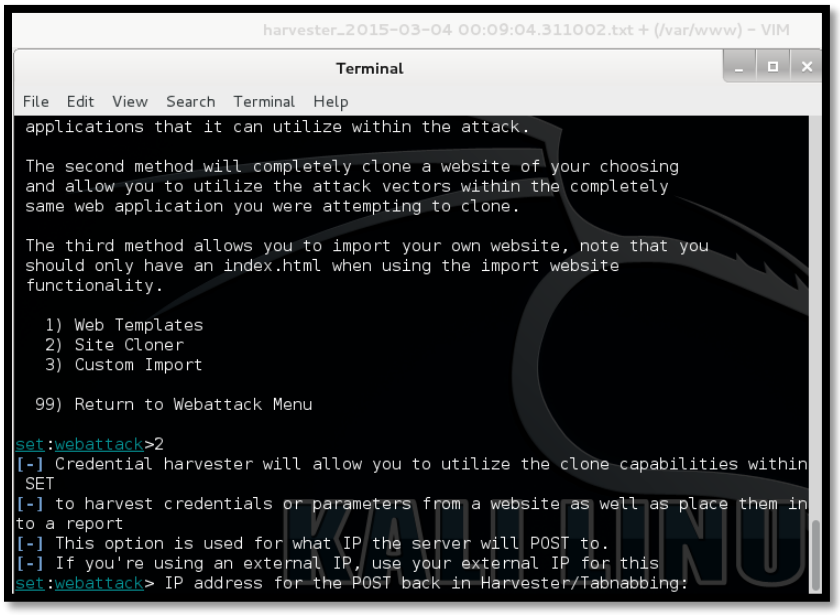
- Una vez seleccionado el vector de ataque, se prosigue con la selección de la recompensa u objetivo de nuestra prueba, en este caso se selecciona la obtención de credenciales de logueo, opción “3- credential harvester attack method”



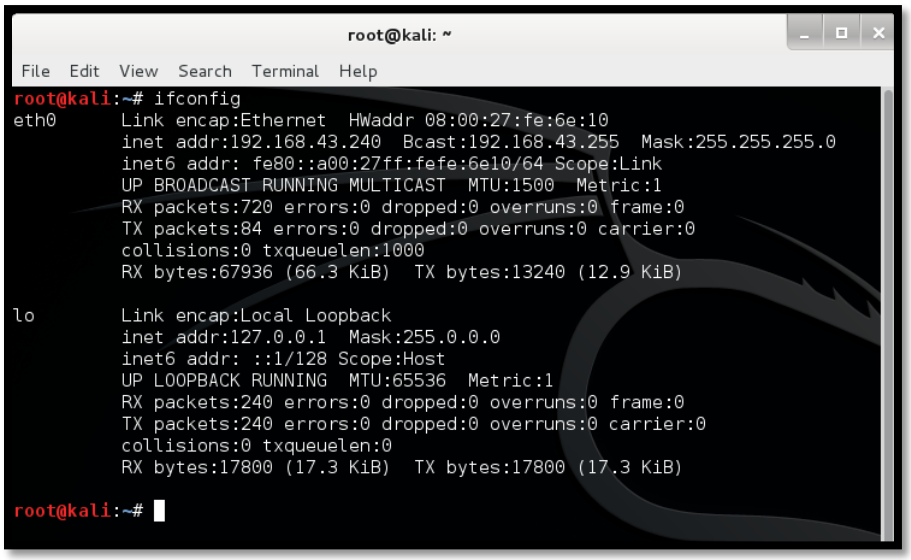

- por último se indica que se va a realizar la clonación de páginas web, para la obtención de credenciales. Esto se realiza por medio de la opción “2- site cloner”



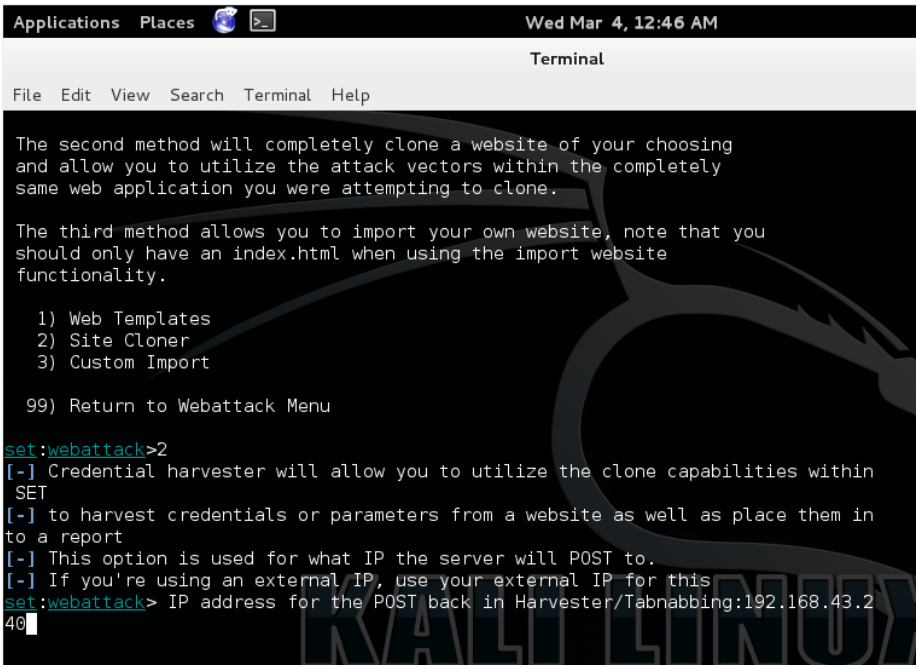

Una vez seleccionado nuestro método de ataque, y recompensa, el paso siguiente consiste en realizar la configuración general del ataque. Para iniciar se requiere conocer la IP de la página la cual funcionara como servidor para alojar la página la cual se va a clonar como lo muestra la siguiente imagen:



Para esto, realizar la consulta de la IP la cual se está utilizando en la maquina virtual, para consultar la dirección IP, se abre una nueva ventana de comando y se realiza la siguiente consulta:

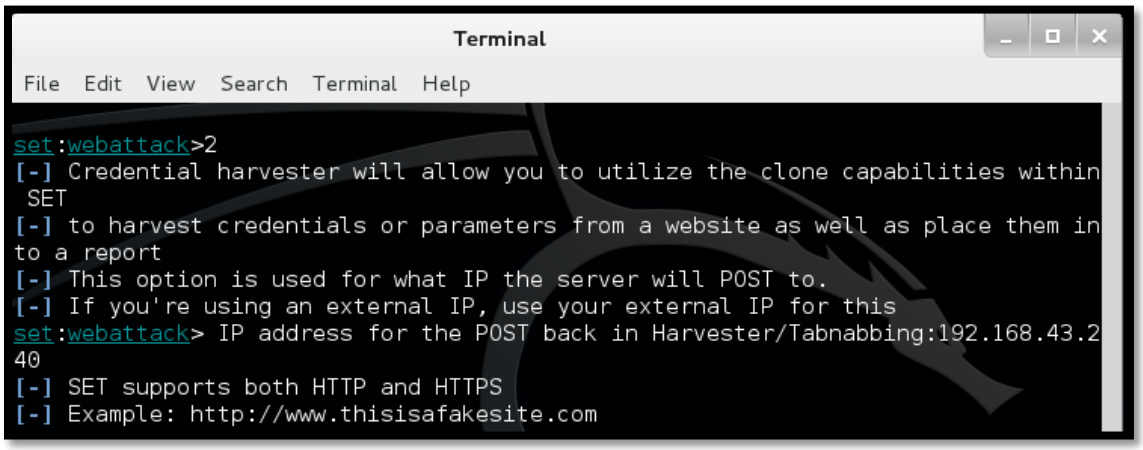



Una vez identificada la direccion IP, se ingresa en la herramienta SET tal cual lo muestra la siguiente imagen:



A continuación el sistema no solicitara la página que se desea clonar, para esto se requiere conocer previamente el sitio web objetivo del ataque e identificar campos de inicio de sesión o campos de texto que se desea obtener. Como el objetivo proactivo y para demostrar el funcionamiento de ataque.

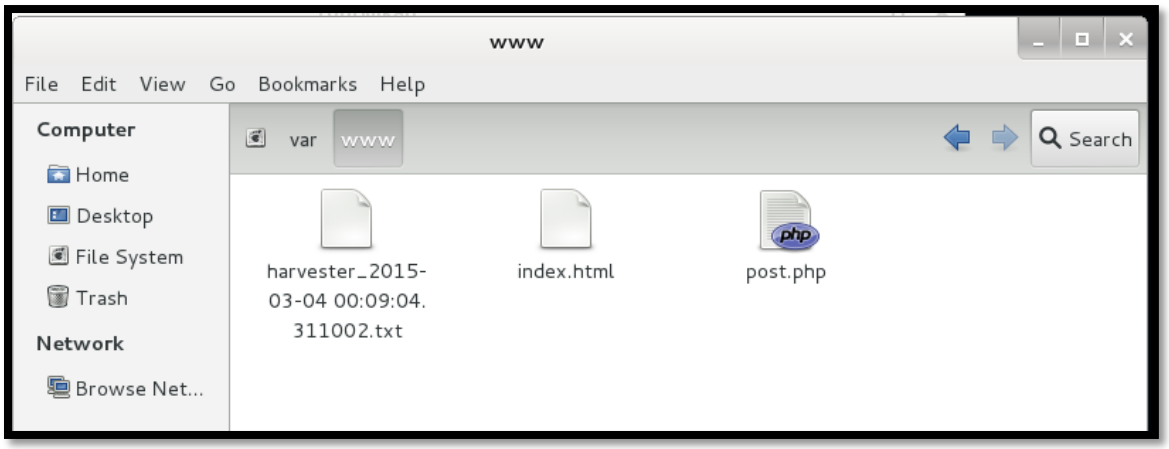
Se ingresa a la página seleccionada tal cual nos indica el aplicativo y se continua para finalizar el proceso de clonación



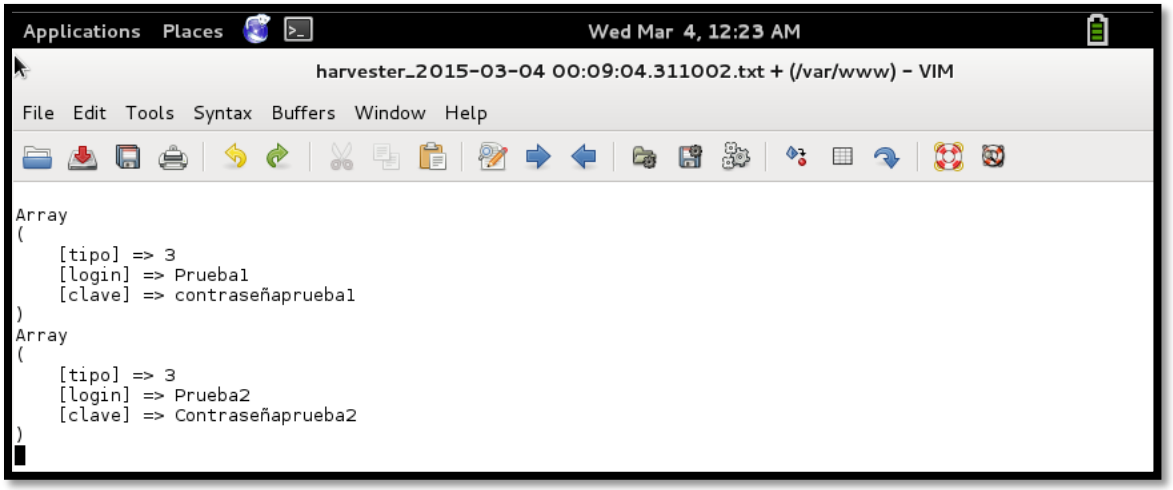

Para probar el funcionamiento de la página clonada, desde cualquier navegador se ingresa la dirección IP del servidor que aloja temporalmente la página clonada el cual se agregó en pasos anteriores. Se observa que no se tienen diferencias entre el sitio real y el sitio clonado. Una vez identificado que no se cuenta con diferencia y que la pagina carga correctamente, se procede a realizar una inserción de dato para probar el funcionamiento de la captura de información. Para esto se ingresa con el usuario Prueba1 y su contraseña contraseñaprueba1.

Al presionar el botón entrar, la herramienta redirigirá al sitio real con el objetivo de poder realizar el logueo de forma correcta evitando sospechas por parte de los usuarios.

Para evidenciar la captura de información, en la consola sobre la cual se esta ejecutando las pruebas se consulta el archivo creado el cual contiene la información registrada en el sitio clonado. Para esto dirigirse a File_system/var/www. El nombre del archivo será: Harvester _año-dia-mes-hora.txt como se muestra a continuación:




Al abrir el archivo observaremos todos los ingresos realizado a nuestro sitio clonado, con la información diligenciada en los campos de texto:




**Preparación del correo Phising:**

Una vez se cuenta configurada la página clon, se requiere definir el método de envió masivo de la página. Cabe aclara que la forma de enviar la página clonada no tiene una metodología específica, está en cada persona el definir un método de envío que se ajuste a sus necesidades, sin embargo a continuación se explicará un método comúnmente utilizado por los hacker alrededor del mundo: el envió de correos de suplantación. Para realizar este correo se requiere:

Información básica del objetivo (persona o empresa) Correo ficticio (puede ser cualquier plataforma gratis: Gmail, Hotmail, zohomail, tce)
El conocer las organizaciones o personas, nos permitirá estructurar un correo que de un grado de confianza a las víctimas, aumentando las probabilidades de éxito de nuestra prueba. Como ejemplos:

- Nombre, teléfono y extensión del director de tecnología con el objetivo de decir que se requiere ingresar al sistema para realizar una actualización

- Nombre, teléfono y extensión del director de recursos humanos, con el objetivo de ingresar al sistema y verificar los datos de información personal

- En caso de personas, conocer sus pasatiempos, hobbies o gustos para estructurar el correo con información que sea de su agrado.

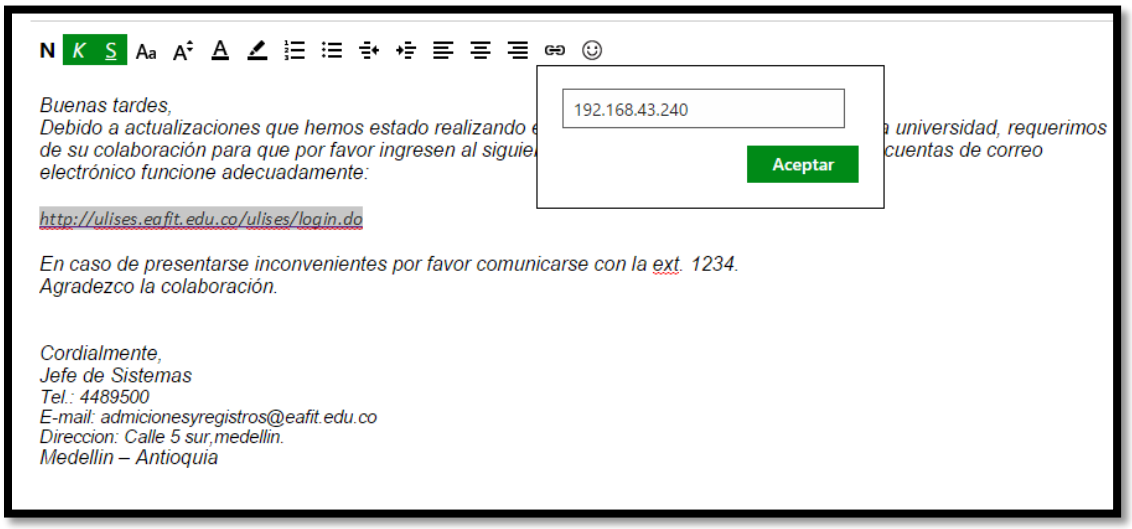
Como se explica anteriormente, las posibilidades para el envío del correo son ilimitadas y cada atacante podrá definir la que más le convenga.
Una vez obtenida la información, se procede a crear la cuenta de correo, para esto se crea, en cualquier plataforma de correo, una nueva cuneta, teniendo en cuenta los datos identificados de la víctima:

Una vez, creada la cuenta se procede con el diseño del cuerpo del correo. Este debe contener una descripción de la actividad ficticia o introducción para contar el objetivo del correo. A continuación un ejemplo:

*"Buenas tardes,*
*Debido a actualizaciones que hemos estado realizando en el servidor de correo electrónico de la universidad, requerimos de su colaboración para que por favor ingresen al siguiente vínculo y verifiquen el acceso a sus cuentas de correo electrónico funcione adecuadamente:*
*http://ulises.eafit.edu.co/ulises/login.do*
*En caso de presentarse inconvenientes por favor comunicarse con la ext. 1234.*
*Agradezco la colaboración.*
*Cordialmente,*

*Jefe de Sistemas*

*Tel.: 4489500*
*E-mail: admicionesyregistros@eafit.edu.co*
*Direccion: Calle 5 sur,medellin.*
*Medellin – Antioquia"*




Una vez diseñada la página, el correo electrónico e identificado la (s) persona(s) u organización víctimas, se rpcoede a ejecutar el ataque enviando el correo electrónico.

El ataque se deja ejecutando por el tiempo que se crea conveniente o hasta cuando se cumpla el objetivo fijado.

**Resultados obtenidos del ataque phishing por clonación:**

Como resultado de la realización de las pruebas de phishing por correo electrónico, se obtendrá las credenciales de acceso a la página atacada de un número determinado de usuarios.

Para el análisis de la los resultados, se realizará una comparación entre la cantidad de empleados que suministraron credenciales de acceso y la totalidad de los correos enviados con el objetivo de determinar el porcentaje de éxito de la prueba. Para esto se realizará la siguiente operación matemática:

$$\left(\frac{a}{b}\right) * 100$$

Donde:

a - será la cantidad de usuarios que suministraron las credenciales de acceso
b - será la cantidad de usuarios a los que se les envió el correo

Dependiendo de los resultados obtenido por la operación matemática se podrá evidenciar que tan fuerte o débil esta la concientización de usuarios respecto a divulgación de usuarios y contraseñas con el objetivo de tomar acciones correctiva.